

On k -Spaces of Real Matrices

ROY MESHULAM

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139

(Received January 27, 1989)

It is shown that if W is a linear subspace of real $n \times n$ matrices, such that $\text{rank}(A) = k$ for all $0 \neq A \in W$, then $\dim W \leq n$. If $\dim W = n$, $5 \leq n$ is prime, and 2 is primitive modulo n , then $k = 1$.

1. INTRODUCTION

Let $M_n(\mathbf{R})$ denote the space of real $n \times n$ matrices. A linear subspace $W \subseteq M_n(\mathbf{R})$ is called a k -space, if $\text{rank}(A) = k$ for all $0 \neq A \in W$. In this note we consider k -spaces of maximal dimension.

THEOREM 1 *The dimension of a k -space $W \subseteq M_n(\mathbf{R})$ is at most n .*

Next we consider an extremal case of Theorem 1. Let $f(n)$ denote the maximal k for which there exists an n -dimensional k -space. A lower bound on $f(n)$ may be obtained as follows:

Let $\rho(n)$ denote the maximal dimension of an n -space of $M_n(\mathbf{R})$. By the Radon-Hurwitz construction, and Adams vector field theorem (see [1]), $\rho(n) = 2^c + 8d$, where $n = (2a + 1)2^{c+4d}$, a, c, d are integers, and $0 \leq c \leq 3$.

Suppose now that A_1, \dots, A_k form a basis of an n -space of $M_n(\mathbf{R})$. Using column notation, we define $W \subseteq M_n(\mathbf{R})$ as the collection of all matrices of the form $[A_1x; \dots; A_kx; 0; \dots; 0]$ where x ranges over \mathbf{R}^n .

Clearly W is an n -dimensional k -space of $M_n(\mathbf{R})$, and hence $f(n) \geq \rho(n) \geq 1$. Equality does not always hold: The skew-symmetric 3×3 matrices form a 3-dimensional 2-space, so $f(3) = 2 > 1 = \rho(3)$.

On the other hand we show:

THEOREM 2 *If $5 \leq n$ is a prime and 2 generates \mathbf{Z}_n^* , then $f(n) = 1$.*

The proofs are topological and are based on a construction of J. Sylvester [5] which associates a bundle map to a k -space of matrices.

2. k -SPACES AND BUNDLE MAPS

Let $\mathbf{P}^{m-1} = \mathbf{S}^{m-1}/\sim$ denote the $m-1$ -dimensional real projective space, viewed as a quotient space of $\mathbf{S}^{m-1} \subseteq \mathbf{R}^m$, under the relation $x \sim -x$. We denote the equivalence class of $x \in \mathbf{S}^{m-1}$ by $[x] \in \mathbf{P}^{m-1}$.

Let γ_{m-1} denote the canonical line bundle over \mathbf{P}^{m-1} , and let $n\gamma_{m-1}$ be the n -fold Whitney sum $\gamma_{m-1} \oplus \dots \oplus \gamma_{m-1}$. The elements of the total space of $n\gamma_{m-1}$ are of the

form $([x], \lambda_1 x, \dots, \lambda_n x)$ where $x \in \mathbf{S}^{m-1}$ and $\lambda_1, \dots, \lambda_n \in \mathbf{R}$. Finally, let ε^n denote the trivial n -plane bundle over \mathbf{P}^{m-1} .

Suppose now that $W = \text{Span}\{A_1, \dots, A_m\}$ is an m -dimensional k -space of $M_n(\mathbf{R})$. As in Sylvester's paper [5], we define a bundle map $f: n\gamma_{m-1} \rightarrow \varepsilon^n$ by:

$$f([x], \lambda_1 x, \dots, \lambda_n x) = \left([x], \left(\sum_{i=1}^m x_i A_i \right) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \right)$$

where $x = (x_1, \dots, x_m) \in \mathbf{S}^{m-1}$.

Since W is a k -space, it follows that f is a mapping of constant rank, hence the image and kernel bundles are defined and satisfy:

$$\text{Im } f \oplus \ker f \cong n\gamma_{m-1},$$

$$\text{Im } f \oplus (\text{Im } f)^\perp \cong \varepsilon^n.$$

Applying the total Stiefel-Whitney classes (see [4]), we obtain the following equalities in $H^*(\mathbf{P}^{m-1}; \mathbf{Z}_2)$:

$$(1) \quad \omega(\text{Im } f) \cdot \omega(\ker f) = \omega(n\gamma_{m-1}) = (1+a)^n,$$

$$(2) \quad \omega(\text{Im } f) \cdot \omega((\text{Im } f)^\perp) = \omega(\varepsilon^n) = 1$$

where $0 \neq a \in H^1(\mathbf{P}^{m-1}; \mathbf{Z}_2)$.

Taking the image of (1) and (2) under the isomorphism $H^*(\mathbf{P}^{m-1}; \mathbf{Z}_2) \rightarrow \mathbf{Z}_2[x]/(x^m)$, it follows that there exist polynomials $p(x), q(x), r(x) \in \mathbf{Z}_2[x]$, $p(0) = q(0) = r(0) = 1$, $\deg p(x) \leq k$, $\deg q(x), \deg r(x) \leq n - k$, such that:

$$(3) \quad p(x) \cdot q(x) \equiv (1+x)^n \pmod{x^m},$$

$$(4) \quad p(x) \cdot r(x) \equiv 1 \pmod{x^m}.$$

Our theorems will follow by considering the above congruences.

Proof of Theorem 1 Suppose W is an m -dimensional k -space of real $n \times n$ matrices. If $m \geq n + 1$ then (3) and (4) imply that $p(x)q(x) = (1+x)^n$ and $p(x)r(x) = 1$. Hence $p(x) = 1$ and so $q(x) = (1+x)^n$, contradicting $\deg q(x) \leq n - k$. Therefore $\dim W = m \leq n$.

Proof of Theorem 2 Suppose now that $5 \leq \dim W = n$, n is a prime and 2 generates \mathbf{Z}_n^* . We shall need the following:

LEMMA (see [2, p. 75]) If 2 generates \mathbf{Z}_n^* , then $1 + \bar{x} + \dots + x^{n-1}$ is irreducible in $\mathbf{Z}_2[x]$. ■

We now consider (3) and (4) with $m = n$.

If $p(x)r(x) = 1$, then $p(x) = 1$ and so, by (3), $\deg q(x) \geq n - 1$. But $\deg q(x) \leq n - k$, hence $k = 1$. Otherwise $p(x)r(x) = 1 + x^n$, $\deg p(x) = k$, $\deg r(x) = n - k$, and hence, by the Lemma, either $p(x) = 1 + x$ and so $k = 1$, or $p(x) = 1 + x + \dots + x^{n-1}$. Since $1 + x + \dots + x^{n-1}$ is coprime to $(1+x)^n$, (3) implies that $q(x) = 1$ and $p(x) =$

$(1+x)^n + x^n$. Therefore

$$\sum_{i=0}^{n-1} x^i = \sum_{i=0}^{n-1} \binom{n}{i} x^i,$$

and so

$$\binom{n}{i} \equiv 1 \pmod{2} \quad \text{for } 0 \leq i \leq n-1,$$

which, by Lucas' Theorem implies that $n = 2^l - 1$ for some l . But then the order of 2 in \mathbf{Z}_n^* is $\leq l < n-1$ contradicting our assumptions. ■

Remarks

1. Theorems 1 and 2 are from the author's thesis [3].
2. Theorem 1 carries over to the complex case using Chern classes. Westwick [6], using the results of [5], has obtained rather tight bounds on the dimension of k -spaces of complex matrices.
3. L. Beasley has recently proved Theorem 1 for arbitrary fields.

References

- [1] J. F. Adams, P. D. Lax and R. S. Phillips, On matrices whose real linear combinations are non-singular, *Proc. Amer. Math. Soc.* **16** (1965), 318–322.
- [2] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, New York, Heidelberg, Berlin, 1982.
- [3] R. Meshulam, Thesis, Hebrew University, Jerusalem, 1987.
- [4] J. Milnor and J. Stasheff, *Characteristic Classes*, Princeton University Press, Princeton, 1974.
- [5] J. Sylvester, On the dimension of spaces of linear transformations satisfying a rank condition, *Lin. Alg. Appl.* **78** (1986), 1–10.
- [6] R. Westwick, Spaces of matrices of fixed rank, *Lin. Multilin. Alg.* **20** (1987), 171–174.